REMARKS

Claims 1-8 remain for consideration. Claims 9-25 have been withdrawn. All claims are thought to be allowable over the cited art.

Claims 9-25 are subject to a restriction requirement. Claim 1 is thought to be generic relative to claims 17 and 18. Furthermore, the apparatus claims 17 and 18 may be used to practice the process of claim 9. Therefore, the restriction requirement is traversed, and reconsideration of the restriction requirement is respectfully requested.

The Office Action fails to show that claims 1-8 are unpatentable under 35 USC §103(a) over the admitted prior art ("APA") in view of "Galovich" (U.S. patent 6,560,709 to Galovich et al.) in view of "Kim" (U.S. patent 6,246,768 to Kim). The rejection is respectfully traversed because the Office Action fails to show that all the limitations are suggested by the references, fails to provide a proper motivation for modifying the teachings of APA with the teachings of Galovich and the teachings of Kim, and fails to show that the combination could be made with a reasonable likelihood of success.

As to claim 1, the combination does not teach a PLD having a plurality of programmable logic resources; a configuration control circuit coupled to the plurality of programmable logic resources; and a key memory coupled to the configuration control circuit and having stored therein a plurality of key bits for defining an encryption algorithm, and at least one bit for indicating whether more keys will follow. The Examiner cites element 12 of Fig. 1 (APA) as corresponding to a key memory. Element 12, however, is configuration memory, not a key memory, and t here is no teaching that configuration memory 12 stores any keys. Note that Fig. 3 of the application, which is not prior art, shows a key memory 23 that is separate from the configuration memory 12. As acknowledged in the Office Action, the APA does not disclose a PLD having stored therein a plurality of key bits for defining an encryption algorithm and at least one bit for indicating whether more keys will follow. In fact, the PLD shown in Fig. 1 does not teach any form of encryption, and thus would have no need for a key memory. Therefore, the APA does not disclose or even suggest a key memory as recited in claim 1.

The Office Action further acknowledges that Galovich does not suggest the limitations of the key memory having stored therein at least one bit for indicating whether more keys will follow, and the Office Action does not show that Kim shows or suggests these limitations.

The Office Action alleges that Kim implicitly discloses indicator bits in the master key to indicate whether more keys will follow. However, Kim has no apparent use for a bit in the master key for indicating whether more keys will follow, and the alleged implication is unsupported by the teachings of Kim. If it were true that Kim implicitly discloses indicator bits, then presumably Kim would suggest how the indicator bits would be used. However, Kim's teachings do not evidence any use for such a bit or bits. Kim's key scheduling device 300 derives from an input 128 bit master key, "sixteen sets of round subkeys, to be used in encrypting the input plaintext data" (col. 2, l. 53). Thus, Kim shows and teaches 16 encrypters and 16 rounds of subkeys. If Kim did imply a bit in the master key for indicating whether more keys follow, there would likely be some explanation of how Kim's disclosed circuitry would operate in response to such bit(s). However, Kim contains no apparent teaching or even suggestion of the claimed bit(s) for indicating whether more keys follow, much less that such bits are stored in a key memory. Thus, the Office Action fails to show that the APA-Galovich-Kim combination teaches all the limitations of claim 1.

The alleged motivation for combining Kim with Galovich is improper. The alleged motivation states that "it would have been obvious ... to employ the use of bit indicating whether more keys will follow, as Kim teaches, in the system of Galovich so as to uniformly assign key values in order to increase the strength of ciphertext data (col. 1, ll. 23-27)." This alleged motivation is not supported by evidence and is therefore, conclusory and improper. Specifically, the Office Action does not provide evidence that Galovich non-uniformly assigns key values or is lacking in the strength of ciphertext data. Furthermore, the alleged motivation is only a general objective and does not suggest modifying Galovich with the specific claim limitations. Thus, the alleged motivation is simply a conclusion and improper.

Moreover, there is no allegation of any motivation whatsoever for combining the APA with either of Galovich or Kim, and Applicants submit that no such motivation

exists in the prior art. Thus, the Office Action fails to establish *prima facie* obviousness with respect to the APA-Galovich-Kim combination, and Applicants respectfully request withdrawal of the rejection. If action other than allowance of the pending claims is to be made and the rejection is maintained, Applicants respectfully requests that the next action be a non-final action explaining the motivation for combining the APA with Galovich and Kim.

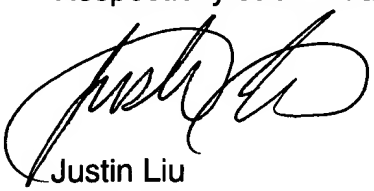
Claims 2, 5, 6, 7, and 8 include limitations that further refine the limitations related to the bit for indicating whether more keys follow. Thus, claims 2, 5, 6, 7, and 8 are thought to be patentable over the APA-Galovich-Kim combination for at least the reasons set forth above. Claims 3 and 4 depend from claim 1 and are also patentable over the APA-Galovich-Kim combination for at least the reasons set forth above.

The rejection of claims 1-8 over the APA-Galovich-Kim combination should be withdrawn because the Office Action fails to show all the limitations are suggested by the combination, fails to provide a proper motivation for combining the references, and fails to show that the combination could be made with a reasonable likelihood of success.

CONCLUSION

Reconsideration and a notice of allowance are respectfully requested in view of the Remarks presented above. If the Examiner has any questions or concerns, a telephone call to the undersigned is invited.

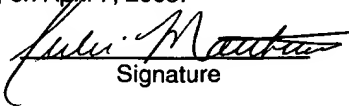
Respectfully submitted,



Justin Liu
Attorney for Applicants
Reg. No.: 51,959
(408) 879-4641

I hereby certify that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on April 7, 2005.

Julie Matthews
Name



Signature